MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2016/2017

TNS3131 – NETWORK SECURITY AND MANAGEMENT

(All sections / Groups)

10 OCT 2016
9.00 a.m. – 11.00 a.m.
(2 hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages of **PART A with 3 questions** and **PART B with 2 questions**.

2. Attempt **ALL questions in PART A** and **ONE out of TWO questions in PART B**. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

PART A – Structured Questions [45 marks]
Answer ALL questions.

QUESTION 1

a) List **FOUR (4)** categories of security attack. State an example for each of the 4 categories of security attack respectively. [4 marks]

b) Define the goal of security services. Describe any **THREE (3)** security services. [4 marks]

c) Using a diagram, label and describe the security model portraying information flowing over an insecure communication channel, in the presence of possible opponents. [3 marks]

d) Define the **TWO (2)** criteria to be met if the encryption scheme is said to be computationally secure. [2 marks]

e) List any **FOUR (4)** Feistel Cipher design elements. [2 marks]

QUESTION 2

a) Compare block cipher and stream cipher in terms of definition and example. [2 marks]

b) Briefly describe the **TWO (2)** major placement of encryption. [2 marks]

c) There are five modes of operation available for use with symmetric block ciphers such as DES and AES.
   i) Besides counter (CTR) mode, briefly describe any **TWO (2)** modes of operation. [2 marks]
   ii) With the aid of a diagram, explain the encryption process for CTR mode. [2 marks]

d) Describe the **TWO (2)** keys used in public-key cryptography. [2 marks]

e) Explain the basic process of enciphering a 64-bit data block using DES with the help of a diagram. [5 marks]

Continued ....

QUESTION 3

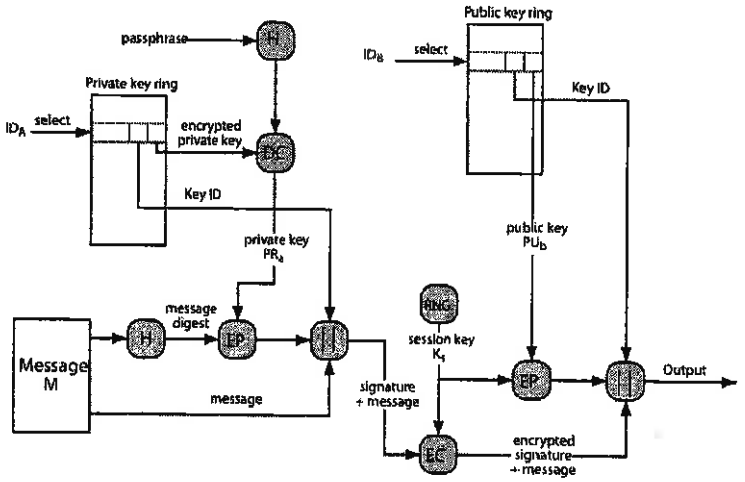
a) Identify the **SIX (6)** message exchange for Kerberos version 4 and 5. [3 marks]

b) Differentiate Kerberos version 4 and 5 in terms of encryption system dependence, message byte ordering, and authentication forwarding. [3 marks]

c) Illustrate the fundamental components of Authentication, Authorization and Accounting (AAA). [3 marks]

d) Given binary input data 00100111 01001100 00010000, identify the character representation for Radix-64 encoding (Refer appendix for Radix-64 table). [3 marks]

e) Given the following diagram for PGP message generation, analyze the message encryption process.



[3 marks]

Continued ....

PART B – Structured Questions [15 marks]
Answer ONE (1) out of TWO (2) questions.

QUESTION 4

a) Describe any **THREE (3)** benefits of IP security when it is implemented in the firewall or routers. [3 marks]

b) Compare transport-mode and tunnel-mode encryption. [2 marks]

c) Explain the difference between SSL and SET. [2 marks]

d) Evaluate if e-commerce transactions are risk-free. [4 marks]

e) Explain the **FOUR (4)** key elements in SNMP. [4 marks]

QUESTION 5

a) Eavesdropping is one of the threats in wireless network.
   i. Describe eavesdropping. [1 mark]
   ii. Explain **TWO (2)** methods to deal with eavesdropping. [2 marks]

b) Application-level gateway is one of the common types of firewalls.
   i. Briefly explain the application-level gateway. [1 mark]
   ii. Describe **TWO (2)** advantages and **ONE (1)** disadvantage of the application-level gateway. [3 marks]

c) Explain the **FIVE (5)** WLAN Vulnerabilities. [5 marks]

d) Network management is an important aspect in networking. List **THREE (3)** key functional areas of network management. [3 marks]

Continued ....

Appendix:

Radix-64 table

6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

End of Paper.